REMARKS

This document is being filed in response to an Office Action mailed 09/09/2004, in which the Examiner said that claims 1-53 were pending but rejected. In this amendment, claims 1, 2. 9, 10, 14, 18, 22, 26, 30, 34, 35, and 49 are amended, and reasons given for rejections are traversed below.

In this amendment, minor grammatical corrections have been made. "And" is inserted where needed in claims 1 and 9 and deleted in claim 30. The punctuation is corrected as needed for consistency within a series in claims 14, 18, 22

Claim 35 is corrected to depend upon claim 34, and claim 49 is corrected to depend upon claim 45.

Claims Rejected under 35 USC §103

Claims Rejected over Baltzley in View of Chandra

In the above-mentioned Office Action, the Examiner said that claims 1-2, 4-14, 16-22, 24-30, 32-32, 40, 42-47 and 49-53 were rejected under 35 USC §103(a) as being unpatentable over U.S. Pat. No. 6,154,153 to Baltzley and further in view of U.S. Pat. No. 4,817,140 to Chandra et al.

Referring to claim 1, the Examiner said that Baltzley teaches...."said server generates a secure transfer key pair and encrypts a private key of said secure transfer key pair [i.e., as depicted in Figure 3 (see associated descriptions for comments)]."

Regarding this statement, the Applicants respectfully submit that, in the disclosure of Baltzley, the descriptions referring to FIGS. 5 and 7 describe the processes occurring within the client machine system of FIG. 2 and the

encryption server of FIG. 3. As described in column 3, lines 32-57, "FIG. 3 shows a diagram of an encryption server comprising incoming and outgoing communication channels, a New User computer program, [and] an Enabler program... FIG. 5 shows a flow chart detailing the functions performed by the New User computer program.... FIG. 7 shows a flow chart detailing the functions performed by the Enabler computer program..." Referring to FIG. 5 and to column 5 of Baltzley, in step 510, the New User program is downloaded from the Encryption Server to the Client Machine. In step 520, a public key/private key pair is generated, and in step 535 the private key is encrypted with a passphrase from the new user, within the Client Machine as the New User program is executed within the Client Machine.

According to the Applicants' invention, a client system is initialized by a process, illustrated in FIG. 3, to operate within the system. In this process a secure transfer key pair is generated within the server, with the private key of the secure transfer key pair being encrypted within the server. On the other hand, Baltzley does not describe this kind of initialization. Instead, the New User program is downloaded to the client, in which a public/private key pair is generated, being encrypted in the client with the user's passphrase.

Thus, the Applicants respectfully submit that Baltzley does not disclose, teach, or otherwise anticipate the requirement of claim 1 for the server to generate a secure transfer key pair and to encrypt a private key of the secure transfer key pair. This requirement is significantly different from the process of Baltzley, in which the key pair is generated and encrypted within the client, since it is much easier to maintain security for the encryption process within the server than in each of a number of client systems.

The Examiner also said that Baltzley teaches that "said transfer key is transferred to each of said client computers in said plurality therfeof with said private key of

said secure transfer key pair in an encrypted form [i.e., the Enabler computer program communicates with the Server computer program to enable a user to both read encrypted messages sent to him or her and send encrypted messages to other users. To read encrypted digital messages sent to the user, the user is first prompted for a passphrase. The passphrase is then hashed and transmitted to the encryption server for authentication. Once the hashed passphrase is authenticated, the encryption server transmits the user's encrypted private key back to the client computer, where it is decrypted. The user may now use the private key to read any digital messages he has received."

However, in the Applicants' invention, the secure transfer key pair is transferred to each of the client systems, with the priv.ate key encrypted, so that each of the client systems is made a part of the system, during the initialization process. Baltzley says nothing of this, instead merely discussing the transmission of a key pair between the client system and the encryption server.

Thus, the Applicants respectfully submit that Baltzley fails to describe, teach, or otherwise anticipate the requirement of claim 1 for the secure transfer key pair to be transferred to each of the client computers in the plurality thereof with the private key of the secure transfer key pair in an encrypted form.

The Applicants further submit that, since Baltzley does not describe the generation of a secure transfer key pair within the server, as described above, Baltzley does not describe the requirements for subsequent use of the requirements related to subsequent use of the secure transfer key pair. Thus, Baltzley does not anticipate the requirement for each client computer to be programmed to generate token data including the portion of the tokey data encrypted with a public key of the secure transfer key pair.

While Chandra teaches teaches the recording of program data on a medium so that the data includes an encrypted portion and an unencrypted portion, as referenced by the Examiner, the Applicants note that Chandra does not include any teachings that make up for the deficiencies of Baltzley in describing the limitations of claim 1, as described above.;

For all the above reasons, the Applicants respectfully submit that claim 1 is patentable under USC §103(a) over Baltzley in view of Chandra.

Regarding claims 2, 7, and 9 the Applicants respectfully submit that the platform key pair required by claim 2 is a second key pair, generated in addition to the secure transfer key pair required by claim 1, which is also required by claims 2, 7, and 9, which depend on claim 1. Thus, the Applicants respectfully submit that Baltzley does not anticipate the requirement of claim 2 for each client computer in the plurality thereof to generate a platform key pair. Additionally, since Baltzley teaches the use of only one key pair, the public key of one key pair cannot be used to encrypt the private key of the other key pair, as further required by claims 2 and 7, or for both of the key pairs to be transmitted over a communications network, as required by claim 7 and 9.

The Applicants further note that adding the disclosure of Chandra does not compensate for the deficiencies of Baltzley in teaching the requirements of claims 2, 7 and 9, as described above.

For all these reasons, the Applicants respectfully submit that claims 2, 7 and 9 are patentable under USC §103(a) over Baltzley in view of Chandra.

Regarding claims 4-6 and 8, the Applicants respectfully submit that, since these dependent claims merely add limitations to claim 1, each of these claims 4-6 and

8 is patentable under USC §103(a) over Baltzley in view of Chandra for reasons described above regarding claim 1.

Regarding claims 10, 18, and 26, the Examiner said:

"i. Baltzley teaches:

(1) receiving a secure transfer key pair; storing said secure transfer key pair [i.e., referring to Figure 3, the private key is then encrypted with the user passphrase yielding an encrypted private key, which is transmitted with the public key to the encryption server 105 for storing (column 2, lines 3537)];

(2) after storing said secure transfer key pair, in response to an indication that token data is to be recorded, encrypting a portion of said token data with a public key of said secure transfer key pair; and recording said token data, including said portion of said token data encrypted with said public key of said secure transfer key pair on a computer readable medium [i.e., the Enabler computer program and the Server computer program also work in conjunction to send encrypted digital messages. Once a digital message is generated, it is encrypted with a client recipient's public key. The encrypted message is then transmitted to the client recipient computer (column 2, lines 49-57)]; and

(3) after storing said secure transfer key pair, in response to an indication that token data is to be read, reading said token data from a computer readable medium, and decrypting a portion of said data with a private key of said secure transfer key pair [i.e., to read encrypted digital messages sent to a user, the user is first prompted for a passphrase. The passphrase is then hashed and transmitted to the encryption server for authentication. Once the hashed passphrase is authenticated, the encryption server transmits the user's encrypted private key back to the client computer, where it is decrypted. The user may now use the private key to read any digital messages he has received (column 2, lines 40-48)]."

In this amendment, claims 10, 18, and 26 are each modified to include a requirement that the computing system referenced in the claim is a client computing system. Claim 10 is additionally modified to include a requirement that the secure transfer key pair must be generated within a server. Claims 18 and 26 include a requirement for the secure transfer key to be received from "said" server, but these claims are modified to replace "said" with "a," since antecedent basis for "said server" is not provided in the claim. Support for these modifications is found in the specification as originally filed on 14, lines 12-13, which describes client systems 10 connected to a server 12.

The Applicants respectfully submit that Baltzley does not teach or otherwise anticipate the requirements of claim 10, as amended herein, for a method in which a client system receives a secure transfer key pair generated within a server, or the requirements of claims 18 and 26, as amended herein, for the secure transfer key pair to be received by a client computer system from a server. Instead, the public/private key pair of Baltzley, described in reference to Fig. 5, is generated within the client system in step 520. This difference is significant, the generation and encryption of the secure transfer key pair within the server of the Applicants' invention allows these processes to be readily made secure, when it may be relatively difficult to secure such processes in each of the client systems.

While Chandra teaches the recording of both encrypted and non-encrypted information on a magnetic media, adding the disclosure of Chandra to that of Baltzley does not make of the deficiencies of Baltzley in describing the limitations of claims 10, 18, and 26, as described above.

Therefore, the Applicants respectfully submit that claims 10, 18, and 26 are patentable under USC §103(a) over Baltzley in view of Chandra.

Regarding claims 11, 19, and 27, Baltzley and Chandra do not anticipate the requirement of these claims for the secure transfer key to be received by the client computer system over a communications network. Instead, as described above in reference to claims 10, 18, and 26, Baltzley teaches that the key pair is generated within the client system. Therefore, the Applicants respectfully submit that claims 11, 19, and 27 are patentable under USC §103(a) over Baltzley in view of Chandra.

Regarding claims 12, 20, and 28, the Applicants respectfully submit that Baltzley and Chandra do not teach, describe, or otherwise anticipate the requirements of these claims for the secure transfer key pair to be subsequently received from the server encrypted with the public key of the platform key pair.

As described by Baltzley in reference to FIG. 5, the encrypted private key and plain text public key are transmitted from the client system to the encryption server to be stored in the encryption server. These keys are not subsequently received by the client system from the server. Therefore, and additionally because claims 12, 20, and 28 merely add limitations to claims 11, 19, and 27, respectively, which are believed to be patentable as described above, the Applicants respectfully submit that claims 12, 20, and 28 are patentable under USC §103(a) over Baltzley in view of Chandra.

Regarding claims 13, 14, 16, 17, 21, 22, 24, 25, 29, 30, 32, and 33, the Applicants respectfully submit that, since claims 13, 14, 16, and 17 merely add limitations to claim 10, since claims 21, 22, 24, and 25 merely add limitations to claim 18, and since claims 29, 30, 32, and 33 merely add limitations to claim 26, these claims 13, 14, 16, 17, 21, 22, 24, 25, 29, 30, 32, and 33 are patentable under USC §103(a) over Baltzley in view of Chandra for reasons described above in reference to claims 13, 18, and 26.

Regarding claims 34 and 44, the Examiner said:

"i. Baltzley teaches:

(1) transferring a secure transfer key pair from said server to said local computer; storing said secure transfer key pair within said local computer [i.e., to read encrypted digital messages sent to a user, the user is first prompted for a passphrase. The passphrase is then hashed and transmitted to the encryption server for authentication. Once the hashed passphrase is authenticated, the encryption server transmits the user's encrypted private key back to the client computer, where it is decrypted. The user may now use the private key to read any digital messages he has received (column 2, lines 38-47)];

(2) establishing communication between said remote computer and said server [i.e., Baltzley's invention provides another important technical advantage by providing a way to securely store a user's private key on an encryption server so a user may access the private key from any client machine on the encryption server network, thus providing roaming capability (column 2, lines 59-63)];

(3) transferring said secure transfer key pair from said server to said remote computer; storing said secure transfer key pair within said remote computer [i.e., to read encrypted digital messages sent to a user, the user is first prompted for a passphrase. The passphrase is then hashed and transmitted to the encryption server for authentication. Once the hashed passphrase is authenticated, the encryption server transmits the user's encrypted private key back to the client computer, where it is decrypted. The user may now use the private key to read any digital messages he has received (column 2, lines 38-47)];

(4) encrypting said portion of said token data within said local computer with a public key of said secure transfer key pair [i.e., once a

digital message is generated, it is encrypted with a client recipient's public key (column 2, lines 51-52)];

(5) recording said token data, including said portion of said token data encrypted with said public key of said secure transfer key pair, within said local computer on a computer readable medium; transporting said computer readable medium from said local computer to said remote computer; reading said token data, including said portion of said token data encrypted with said public key of said secure transfer key pair, within said remote computer from a computer readable medium; decrypting said portion of said token data within said remote computer with a private key of said secure transfer key pair; and enabling said performance of said predetermined task in said remote computer in response to said portion of said token data [i.e., as depicted in Figures 5 and 7 (see associated descriptions for details in column 5, lines 8-61 and column 6, line 53 through column 7, line 11; and column 2, lines 38-48)]."

In this amendment, claim 34 is modified to include a requirement that the secure transfer key pair must be generated within a server. Support for this modification is found in the specification as filed on page 8, lines 24-25, on page 18, lines 22-24, and on page 20, lines 16-19. This requirement has also been included, for example, in claim 1 as initially filed. Claim 44, as filed, includes a requirement that the secure transfer key pair must be generated within a server.

The Applicants respectfully submit that Baltzley does not teach or describe the requirement of claim 34, as amended herein, and of claim 44, for the secure transfer key pair to be generated within the server. The key pair described by Baltzley as cited by the Examiner is generated within the client system in step 520 and encrypted within the client system in step 535 before being transmitted to the server in step 540. The differences and advantages of the Applicants' method of generating the secure transfer key pair within the server instead of within the client system are significant. The process of generating and

encrypting the password is much more easily secured when it is confined to the server. Furthermore, with the Applicants' method, all of the client systems that are to perform certain functions share a common secure transfer key pair, part of which is encrypted for the use of the particular client system. In the Applicants' system, this secure transfer key pair does not change when a new user is added; in the system of Baltzley, a new key pair is added for each new user.

Furthermore, the Applicants respectfully submit that Baltzley does not teach or describe the requirement of claim 34 for transporting the computer readable medium from the local computer to the remote computer or the requirement of claim 44 for transferring the computer readable medium from the first client computer to the second client computer. Transporting or transferring the computer readable medium is not the same as transmitting the data over a communications channel. Baltzley does not mention transporting a computer readable medium from one client system to another. This difference is also significant, since an objective of the Applicants' invention is to provide the user with a token in the form of a computer readable medium to take from one client system to another so that certain functions can be performed.

While adding the disclosure of Chandra to that of Baltzley provides anticipation for the recording of encrypted and unencrypted data on a computer readable medium, the deficiencies described above relative to the anticipation of elements of claim 34 remain.

For these reasons, the Applicants respectfully submit that claim 34, as amended herein, and claim 44 are patentable under 35 USC §103(a) over Baltzley in view of Chandra.

Regarding claims 35-38, 40, 42, 43, 45-47 and 49 the Applicants respectfully submit that, since claims 35-38, 40, 42, and 43 merely add limitations to claim

34, and since claims 45-47 and 49 merely add limitations to claim 44, these dependent claims are all patentable under 35 USC §103(a) over Baltzley in view of Chandra for reasons described above regarding claims 34 and 44.

Regarding claim 50, the Applicants respectfully submit that Baltzley and Chandra do not teach or anticipate the requirement of this claim for generating a secure transfer key pair within a server, for reasons described in detail above regarding claims 34 and 44.

Furthermore, the Applicants respectfully submit that do not teach or anticipate the requirement of claim 50 for transferring the secure transfer key pair from the server to each client computer within the plurality of client computers. Instead, in the system of Baltzley, a key pair is transferred only when the user provides an input at the client; there is no instance of a key pair being transferred to all of the client computers in the system.

For these reasons, the Applicants respectfully submit that claim 50 is patentable under 35 USC §103(a) over Baltzley in view of Chandra.

Regarding claims 51-53, since these dependent claims merely add limitations to claim 50, the Applicants respectfully submit that claims 51-53 are patentable under 35 USC §103(a) over Baltzley in view of Chandra for reasons described above regarding claim 50.

Claims Rejected over Baltzley in view of Taaffe

In the above mentioned Office Action, the Examiner said that claims 3, 15, 23, 31, 39, 41, and 48 were rejected under 35 U.S.C. 103(a) as being unpatentable over Baltzley (US 6,154, 543), and further in view of Taaffe (US 4,747,139).

Regarding claim 3, the Examiner indicates that Taaffe describes the requirement of this claim for a security subsystem generating a hardware key pair and providing encryption and decryption. However, the Applicants respectfully submit that, since Taaffe does not describe a system exchanging key pairs with a server, including the disclosure of Taaffe to that of Baltzley in describing the limitations of claims 1 and 2, upon which claim 3 depends. Therefore, for reasons described above regarding claims 1 and 2, the Applicants respectfully submit that claim 3 is patentable under 35 USC §103(a) over Beltzley in view of Taaffe.

Regarding claims 15, 23, and 31, the Examiner indicates that Taaffe describes the requirement of this claim for a security subsystem generating a hardware key pair and providing encryption and decryption. However, the Applicants respectfully submit that, since Taaffe does not describe a system exchanging key pairs with a server, including the disclosure of Taaffe to that of Baltzley in describing the limitations of claim 10, upon which claim 15 depends, of claim 18, upon which claim 23 depends, and of claim 26, upon which claim 32 depends. Therefore, for reasons described above regarding claims 10, 18, and 23, the Applicants respectfully submit that claims 15, 23, and 31 are patentable under 35 USC §103(a) over Beltzley in view of Taaffe.

Regarding claims 39, 41, and 48, the Examiner indicates that Taaffe describes the requirement of this claim for a security subsystem generating a hardware key pair and providing encryption and decryption. However, the Applicants respectfully submit that, since Taaffe does not describe a system exchanging key pairs with a server, including the disclosure of Taaffe to that of Baltzley in describing the limitations of claim 34, upon which claims 39 and 41 depend, and of claim 44, upon which claim 48 depends. Therefore, for reasons described above regarding claims34 and 44, the Applicants respectfully submit that claims

39, 41, and 48 are patentable under 35 USC §103(a) over Beltzley in view of Taaffe.

Conclusions

The Applicants respectfully submit that the application, including claims 1-53 is now in condition for allowance, and that action is respectfully requested, with reconsideration and withdrawal of all reasons given for rejections.

Respectfully submitted,

Ronald V. Davidge

December 9, 2004